applicable to configurations where a single or a small number of servers provide service to a large number of clients. In particular, if a server were to widely distribute an identifier to multiple clients, an imposter server could easily intercept the identifier and attempt to adopt the identity of the authorized server.

In addition, the entity that desires to control access by unauthorized servers is often not the client, but is instead the operator of the authorized server. When an unauthorized server attempts to gain access to client systems, the operator of the authorized server may not be aware of the attempt. Accordingly, if conventional security systems were the only available means of protection, the client system and the operator of the unauthorized server could collude to override the security system. As a result, any security system that is freely accessible by the operators of client systems or unauthorized servers could be breached relatively easily.

In view of the foregoing, what is needed is a system for verifying the identity or authorization of servers to provide network resources to client systems. It would be an advancement in the art to provide a system for verifying the authorization of servers that is not merely analogous to the conventional use of identifiers to verify the identity of clients. It would be particularly advantageous to verify the authorization of servers using a security system that cannot be readily accessed or overridden by an operator of the client system. It would also be desirable to combine such a system for verifying the authorization of servers with a system for verifying the identity of clients.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

SUMMARY AND OBJECTS OF THE INVENTION

The present invention relates to systems and methods for verifying the authorization of a server to provide network resources to a client. The authorization process requires the server to decrypt a message generated by the client and to respond with an appropriate encrypted message. Authorized servers have the decryption key needed to decrypt the message, whereas unauthorized servers will be unable to decrypt the message or to return the appropriate encrypted message to the client. The system can be configured to prevent software operating on the client from enabling the functions of the client without proper server authorization or may otherwise override the security features. In addition, the process of verifying the authorization of the server can be combined with measures to verify the identity of the client.

According to one implementation of the invention, when a security counter, or timer, exceeds the value of an expiration count stored at the client or at other selected times, an authorization interrupt is generated. The other selected times for generating authorization interrupts may occur, for example, when the client is turned on or when software operating at the client generates a reauthorization signal. The authorization interrupt eventually disables some or all of the functions of the client unless the server is authorized within an allotted period of time. In response to the authorization interrupt, the client generates a client message that includes the value of the security counter, a client identifier, and a random number. The client message is encrypted using an encryption key and is transmitted to the server.

If the client message is received by an unauthorized server, the server is unable to decrypt the message and to access the encoded information included therein. When the client message is instead received by an authorized server, the server uses a decryption key

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

to decrypt the message. The server then decombines the value of the security counter, the client identifier, and the random number. Based on the value of the security counter, the server selects a new expiration count that will cause the client to again initiate the authorization process at a future time. The client identifier is compared against a client authorization database to determine the level of service that the client is authorized to receive. The level of service represents a level of functionality that the client is permitted to exhibit. The server generates an authorization code corresponding to the authorized level of service.

The server then creates a service message by combining the new expiration count, the authorization code, and the random number that was included in the client message. The server encrypts the service message and transmits it to the client. If the client message had been received by an unauthorized server, the message would have remained encrypted, such that the unauthorized server would not have gained access to the random number. Thus, any service message created by an unauthorized server will not include the original random number.

The client receives, decrypts, and decombines the service message. The random number included in the service message is compared with the random number included in the client message. If the random numbers are the same, the client assumes that the server is authorized to provide network resources. The new expiration count is written to an expiration count register and the new authorization code is written to an authorization register at the client. The client can then receive service from the server until the security count exceeds the new expiration count. If, however, the random numbers are not the same, the client assumes that the server is unauthorized, and the functions of the client are disabled according to the authorization interrupt after the allotted time has expired.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111